tyco Tyco Valves & Controls, LP

PENBERTHY®

yarway

320 Locust Street
Prophetstown, IL 61277-1147
Voice: 815-537-2311 x160
Fax: 815-537-5764
e-mail: gsanders@tycovalves.com
Fri - 29 Oct 04

PenTech FAQ # 12 by Gary G. Sanders, Director of Engineering

Failsafe, Pump Control and other Instrumentation Logic

I was recently asked to define failsafe and pump control logic for someone new to instrumentation and provided a basic answer. Shortly thereafter I went to the reference library for a more precise definition. After “index chasing” seven classic text / reference / handbook volumes on instrumentation and / or control, I was surprised to find that this ‘commonly used’ term [failsafe] was not to be found. Any editors / contributing authors, especially to glossary or definition sections, please take note.
I paraphrase the closest item I found, 'a process condition that can be characterized by defining either the presence or absence of an electrical signal'. In my opinion, this is not a very satisfactory answer.

Failsafe

A failsafe condition exists when the power is off (the base or default state). An example is a de-energized relay coil. Failsafe output for instrumentation is an output conditioned such that the parameter of interest in warning / alarm / fault mode or any failure (system, circuit, power, etc.) causes the output state to go to the default state. It is based on classic relay logic assuming that in the normal (non-fault) operating state power will be supplied and the relay coil will be energized. This means that parameter warning mode or essentially any system failure, including power loss, will cause a change of state, i.e.; coil de-energized. For failsafe operation, instrumentation designers must configure their circuitry to energize the relay coil when conditions are normal.

Consider a high liquid level switch: As vessel filling exceeds the switch point, the parameter of interest, the liquid level, will cause an output state change. Many people tend to think that this condition should cause the instrument to turn something on – like a light switch. Considering a relay as the output device, if wired like a light switch, the normally open relay contacts would close as the relay coil was energized and the armature pulls in. This means the instrument supplies power to the relay coil as its switch point is exceeded. The problem with this scenario is other failure modes, such as; power loss, most instrument failures, etc. could never cause a fault output. Thus in a failsafe system, these conditions are internally inverted. The expected relay contact change occurs as the switch point is exceeded; this change of state causes the coil to be de-energized, the relay armature drops out and the NC contacts close.

To complete the failsafe state, the user output must be wired through the normally closed (NC)(coil de-energized) set of contacts. This completes a double inversion and provides active alarm upon activation. When the setpoint is not exceeded (normal operation), the relay coil is energized by the instrument and these contacts are open. When the process exceeds the setpoint, the relay de-energizes and the normally closed contact set closes. Of course, the contact set will also close if the instrument loses power or if there is a circuitry failure in a properly designed instrument. Alarm output is thus established in any of these three modes.

For level measurement, most single point switches are universal. They may be applied as high or low level alarms. The instrument typically employs a set-up switch or jumper to select either high or low level switching. Remember that [failsafe] high level and low level alarms are opposite acting, therefore they should not be set up the same way.

Naming Conventions

Failsafe naming conventions refer to the parameter of interest and / or its fault (alarm) condition. In the liquid level applications referred to previously, the parameter of interest is always the liquid level (therefore not usually redundantly mentioned) and the alarm condition. For example, a low level sensor becomes low level failsafe when its output goes to default mode when in the alarm state, in this case liquid lower than the sensor. The situation gets more complex if there is more than one parameter of interest. Consider a boiler system: depending on application, either the presence or absence of water or steam may be the parameter of interest. If the sensor assignment is to go to the default state upon detection of low drum water level (loss of water is the parameter of most interest) it is called 'water failsafe'. If the sensor is applied to detect loss of steam in a drip leg of a turbine feed system, it is called 'steam failsafe' (consider TWIP [turbine water induction prevention] applications).

Pump Control

Pump control comes in two variations: pump up (a.k.a. pump in) and pump down (a.k.a. pump out). Pump up means filling a vessel when the low level sensor is activated and turning off the pump when the high level sensor is exceeded. Pump down is emptying a vessel when the high level switch turns on the pump and the low level switch shuts it off.

Consider two level switches (wired failsafe), one high and one low. The high level setpoint will change output state when the fill level exceeds the sensor position. The low level will change output state when fill level is below its setpoint. Rhetorical - does this imply that a pump may be directly wired through the two relays to operate the pump?

Consider pump up conditions: Liquid level in the vessel falls below the low level switch setpoint. It changes output state which is wired to turn on the pump. As soon as sufficient refilling occurs to exceed the level of this same low level switch it reverses output state and the pump turns off. Depending on system hysteresis, this short cycling around the low level switch will continue. The level will never vary far from the low level sensor and has no chance of approaching the high level sensor position. When the low level switch changes output state and starts the pump, obviously what is required is a mechanism (called a latch - it holds the last input until a different input releases it) to maintain the pumping operation until the high level switch changes its output state. In latching relay logic terms, connect the armature coil to the low level switch and the ratchet release coil to the high level switch. A digital logic latch works on exactly the same principal. All TV&C-Prophetstown products (except the conductance product line) that have dual (or more) sensing points incorporate the selection of either level sensing with two points (individually programmable for high or low level) or pump control (programmable for either pump up or pump down logic). If two electrically separated switches (setpoint only) are used (e.g.; on a magnetically coupled liquid level gage or the conductance product line) then a separate pump control logic module is available as an option.

High-High and Low-Low

Once the selection of pump control or standard setpoints has been addressed, sometimes there is a requirement for overflow or pump dry protection in case the primary control system is somehow bypassed. Overflow sensors in these applications are termed high-high setpoints and are usually wired to scram (emergency shutdown action) the process. The equivalent low-low prevents, for example, a dry suction line to a pump.

Timed Cascade

Sometimes a setpoint is so critical that even approaching it presents a potentially perilous situation. Typically, three sensors (systems exist with 2 to n sensors) are closely arrayed with the last being at the critical point, the others are arrayed toward the normal operating domain. When the sensor farthest from the critical point is triggered a timer (counter or accumulator) is started. When the next sensor is triggered, another faster input to the timer (counter or accumulator) is added. Finally when the critical point is triggered, output state change is instantaneous. If only the first or second sensor is triggered then the output will change state at the time out interval selected. On some systems a warning is also given that indicates that the time out sequence has been initiated.

Majority Logic or Voting

In processes where a reasonable possibility of sensor fouling exists, three or more sensors are arrayed similar to the timed cascade. However, the sensors are usually physically closer to each other or are on the same plane. The logic concept is that a majority (2 of 3, 3 of 4, 3 of 5, 4 of 6, etc.) of the sensors must change state (democratically vote) before the final output state will change.

Unanimous Logic

When setpoints are used for scramming an entire process or plant, multiple sensors are sometimes logically AND'ed (all inputs must be true for a true output) before a scram output is generated (scram recovery costs are high). Typically 3 to 5 cascaded sensors are used with the final trip occurring at the critical process point. The application for this logic is usually systems that normally incorporate multiple sensor locations, for example, boiler water level conductivity systems. The purpose of unanimous logic is to avoid false trips - but if one of the critical sensors is not operating properly it can be dangerous. Majority logic is superior since it makes allowance for inoperative sensor(s), the only drawback is the possibility of occasional false trips.

1 of N Logic

If switching does not require precision (i.e.; switching is allowed in a general area, not at a specific geometric point) in processes where a reasonable possibility of sensor fouling exists, two or more sensors may be logically OR'ed (any one or more true inputs yields a true output). If any one changes output state, the logical output will also change output state.

Other Logic

With combinational logic many different (some very complex) algorithms are possible, for example, the level error signal on Penberthy Model 12B or Yarway Model 3000 is generated by combinational logic. The most common logic types have been addressed in this FAQ.

Acknowledgements to Larry Fetterolf, Baton Rouge, LA and Dave Wiersema, Fulton, IL for advocating the inclusion of this subject in the FAQ series.

Copyright © 2004 TV&C - Prophetstown, All Rights Reserved